

The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project

by LUCIANA DURANTI and HEATHER MACNEIL

Résumé

Le projet de recherche en cours au Programme de maîtrise en études archivistiques de l'Université de la Colombie-britannique vise à identifier et à définir les conditions requises pour la création, la manipulation, et la sauvegarde de documents informatiques sûrs et authentiques. Cet article brosse un tableau du projet de recherche en soulignant ses objectifs et sa méthodologie, en résumant son analyse conceptuelle, et en présentant ses principales conclusions.

Abstract

The research project currently underway at the University of British Columbia's Master of Archival Studies Programme is directed toward identifying and defining the requirements for creating, handling, and preserving reliable and authentic electronic records. This article provides an overview of the research project, outlining its objectives and methodology, summarizing its conceptual analysis, and presenting its major findings to date.

It is generally recognized that, while computer technology makes the production, transmission, manipulation, organization, maintenance, and consultation of records easier, faster, and cheaper, it also represents a threat to their integrity, accessibility, and preservation. The difficulties associated with making and keeping trustworthy records in electronic form provided the justification for a three year Social Sciences and Humanities Research Council of Canada (SSHRC) funded research project which began in April 1994 and which will conclude in March 1997. The research project, which is being carried out by a research team from the Master of Archival Studies Programme at the University of British Columbia,¹ "aims to identify and define in a purely theoretical way both the byproducts of electronic information systems and the methods for protecting the integrity [meaning the reliability and authenticity] of those which constitute evidence of action."² The objectives of the research project are:

- to establish what a record is in principle and how it can be recognized in an electronic environment;
- to determine what kind of electronic systems generate records;
- to formulate criteria that allow for the appropriate segregation of records from all other types of information in electronic systems generating and/or storing a variety of data aggregations;
- to define the conceptual requirements for guaranteeing the reliability and authenticity of records in electronic systems;
- to articulate the administrative, procedural, and technical methods for the implementation of those requirements; and
- to assess those methods against different administrative, juridical, cultural, and disciplinary points of view.³

At the conclusion of the project, the final findings of the research will be examined in detail in a monograph illustrating as well the project's methodology and hypotheses. The purpose of the present article is threefold: firstly, to outline the methodological framework of the research project; secondly, to summarize the conceptual analysis of *records*, *reliability*, and *authenticity* that formed the core of the research; and, thirdly, to present the project's major findings deriving from that conceptual analysis, while suggesting some of their broader implications for the archival management of electronic records.⁴

The methodological approach of the research project was primarily deductive, that is, it began with a set of general premises about the nature of records and then examined those premises to determine whether they were supportable in an electronic environment. The theoretical basis for the general premises concerning the nature of records and the conditions necessary for ensuring their trustworthiness were the principles and concepts of diplomatics, which studies records as individual entities, and archival science, which studies records as aggregations. Diplomats is a body of concepts and methods, originally developed in the seventeenth and eighteenth centuries, "for the purpose of proving the reliability and authenticity of documents." Over the centuries, it has evolved "into a very sophisticated system of ideas about the nature of records, their genesis and composition, their relationships with the actions and persons connected to them, and with their organizational, social, and legal context."⁵ Archival science, which emerged out of diplomatics in the nineteenth century, is a body of concepts and methods directed toward the study of records in terms of their documentary and functional relationships and the ways in which they are controlled and communicated. During the course of the research, the principles and concepts of diplomatics were integrated with those of archival science and interpreted within the framework of electronic systems. This conceptual analysis generated a number of hypotheses expressing the necessary and sufficient components of a complete, reliable, and authentic electronic record. These hypotheses, which have been articulated in templates,⁶ constitute the conceptual basis for establishing, firstly, whether a given electronic system contains records and, secondly, whether these records can be considered reliable and authentic.

In order to translate the hypotheses into functional requirements for the creation, handling, and preservation of reliable and authentic records, it was necessary to explicate those concepts in implementable terms. It was fortunate, therefore, to find that the U.S. Department of Defense Records Management Task Force (DoDRMTF) was actively seeking a theoretical foundation for its re-engineering effort. The DoDRMTF contributed to the UBC-MAS research methodology its own standard modelling technique, Integrated Definition language (IDEF), which was useful for the purposes of analyzing and graphically representing the diplomatic and archival concepts, and making their meaning comprehensible and relevant to system designers. The templates developed by the UBC-MAS research team provided the concepts to be represented, while IDEF provided the means of translating those concepts into activity and entity models that show the relationships of their components from well identified viewpoints⁷ and for determined purposes. For the aims of the UBC-MAS research project, the viewpoint chosen was that of the record creator and, more specifically, a corporate body, primarily because of the project's focus on reliability and authenticity. The activity models define all the activities associated with the records management function. That function has been labelled **MANAGE ARCHIVAL FONDS** and it includes all the activities associated with the creation, handling, and preservation of active and semi-active records. The entity model defines all the entities associated with those activities, e.g., **OFFICE, CLASS, PROCEDURE, DOSSIER, RECORD**, as well as their attributes (i.e., characteristics or properties) and the relationships between and among them. The activity and entity models describe the creation, handling, and preservation of an agency's records, both electronic and non-electronic. On the basis of the activities identified in the models, the research team, in collaboration with the DoDRMTF, has also developed detailed rules for creating, handling, and preserving those records.⁸

Before proceeding to the conceptual analysis of records, which constituted the core of the research, it is necessary to explain briefly the records management framework in which that analysis has been situated. The diplomatic and archival principles and concepts that have been elaborated and interpreted for the purposes of the research project function as standards for the design of recordkeeping and record-preservation systems, and for the evaluation of the records produced, used, maintained, and preserved over the long term in electronic form. A *recordkeeping system* comprises a set of internally consistent rules that govern the making, receiving, setting aside, and handling of active and semi-active records in the usual and ordinary course of the creator's affairs, and the tools and mechanisms used to implement them. In other words, *recordkeeping* is "keeping record of action": as such, it is the presupposition for the existence and the first object of *records management*, which is the management over time, from the creator's perspective and for its purposes, of the creator's records, of the means used to control their creation (e.g., classification, registration, and retrieval instruments), and of the human, technological, and space resources necessary to their handling, maintenance, and preservation. Although the management is from the perspective of the creator and for its purposes, it serves broader social aims that go beyond the carrying out of specific affairs, encompassing legal requirements, administrative accountability, social accountability, and historical accountability. The *record-preservation system* is a set of internally consistent rules that govern the intellectual and physical maintenance by the creator of semi-active and inactive records

over time, and the tools and mechanisms necessary to implement them.⁹ The *records system* of the creator thus comprises the creator's records, and its recordkeeping and record-preservation systems, and is controlled by the creator's records management function.

Within the framework just described, the conceptual analysis of records focused on the definition of three key terms: *record*, *reliability*, and *authenticity*. The research team began its work by identifying and defining the components of a record in a traditional and in an electronic environment using concepts derived primarily from diplomacy. At the heart of diplomacy lies the idea that all records can be analyzed, understood, and evaluated in terms of a system of formal elements that are universal in their application and decontextualized in nature. This implies that records can and must be identified by their formal constituents, and not by the information they convey. Diplomatic examination shows that an electronic record, just like every traditional record, is comprised of *medium* (the physical carrier of the message), *form* (the rules of representation that allow for the communication of the message), *persons* (the entities acting by means of the record), *action* (the exercise of will that originates the record as a means of creating, maintaining, changing, or extinguishing situations), *context* (the juridical-administrative framework in which the action takes place), *archival bond* (the relationship that links each record to the previous and subsequent one and to all those which participate in the same activity), and *content* (the message that the record is intended to convey). However, with electronic records, those components are not inextricably joined the one to the other, as in traditional records: they, and their parts, exist separately, and can be managed separately, unless they are consciously tied together for the purpose of ensuring the creation of reliable records and the preservation of authentic records.

With electronic records, the **medium** is a separate physical part of the record, which is not meant to convey meaning, but whose exclusive purpose is to provide a support for the message. While a record does not come into existence until it is affixed to a medium, the neutral character of the medium in electronic records is vital to their survival, because all media designed to carry magnetically or optically affixed signals have very limited longevity, due not only to the deterioration of the material, but also, and primarily, to the obsolescence of the technology necessary to read them. The obvious implication is that the preservation of electronic records requires repeated and continuing reproduction. If the medium were meant to convey meaning *per se*, each reproduction would be a simple transcription of the content, with notable loss of information and authority. However, because the medium of electronic records is not imbued with meaning, each record reproduction in which the only component that changes is the medium can be taken to be a complete and effective record identical to the one that it reproduces.

A similar issue arises with the group of record characteristics that constitute its **physical form**. Physical form comprises the formal attributes of the record that determine its external make-up. It includes script (type font, format, inserts, colours, etc.), language, special signs (symbols indicating the existence of attachments or comments, mottoes, emblems, etc.), seals of any kind (including digital signatures, time-stamps, etc.), the configuration and architecture of the electronic operating system, the architecture of electronic records, the software, etc., that is, all those

parts of the technological context that determine what the document will look like and how it will be accessed, and that, in electronic systems, are mostly “transparent,” or invisible, to the user (whoever the user might be, author, addressee, or other).

Because the components of the physical form of a record are intended to convey meaning, any change in any of them generates a new and different record. This again has implications for the preservation of electronic records. Digital technology becomes obsolescent every few years, that is, radical changes take place in the configuration and architecture of electronic systems, such as the shift from a flat file concept to a hierarchical or a relational database concept. When this happens, all records generated in the obsolescent environment must be migrated to the new one, otherwise they will become inaccessible and, for all purposes and consequences, non-existent. Migration is different from copying, in that the latter is a complete reproduction of both the content and formal elements of the records (e.g., microfilming, photocopying, or transferring the same strings of bits from a magnetic tape to another), while the former is a reproduction of the content of the record, with changes in configuration and structure (e.g., imaging of analog records, or transferring of hypertext records from one database to another having a different configuration). While, after migration, the resulting records may look like the ones that have been migrated, their physical form has substantially changed, with loss of information on the one hand, and addition of new information on the other hand.

All the above implies that every process of migration must be self-authenticating. If the records are still needed by the record creator for the usual and ordinary conduct of its business, the continuing reliance of the creator on the products of the migration process by itself authenticates them. If the records are no longer needed by the record creator in the course of its business, the migration process will have to be carried out by a neutral party (e.g., a professional archivist employed by the institution or programme that is competent in the permanent preservation of the records in question), and its products will need to be verified and authenticated: they would thus become authentic copies¹⁰ of the obsolescent records, at best imitative¹¹ (if an effort is made to reproduce their intellectual form), and at worst *simple copies* with the nature of a *vidimus*.¹²

The **intellectual form** of a record is the sum of its formal attributes that represent and communicate the elements of the action in which the record is involved and of its immediate context, both documentary and administrative. The intellectual form of electronic records may be subdivided into three parts: the “information configuration,” which refers to the type of representation of the content, whether text, graphic, image, sound, or a combination thereof; the “content articulation,” which refers to the elements of the discourse and their arrangement, such as date, salutation, exposition, etc.; and “annotations,” which refer to the additions made to the record either in the execution phase of the procedure (e.g., authentication of signatures), or in the handling of the matter (e.g., indication of “urgent” or “bring forward,” date and name of action taken), or in the development of the procedure (e.g., mention of subsequent actions or their outcome), or in the management of the record (e.g., classification code, registry number).

Content articulation includes primarily elements that, in traditional documents, are called “intrinsic.” With electronic records that are transmitted across electronic boundaries, the most important of those elements, that is, those referring to persons, administrative context, and action (e.g., superscription,¹³ inscription,¹⁴ date of document, date of transmission, subject), are in the header of the record, which is its protocol,¹⁵ not in the eschatocol¹⁶ of the record, which may contain mention of names, but without any validity as attestations of what the record is all about. With records that are not transmitted across electronic boundaries, those same elements may be mentioned in the content articulation, but they have validity as attestations of what the record is about only if they appear in the record profile.

Annotations include the “record profile,” which is an electronic form that is generated when the order is given to the system to send or to close an electronic record. As an annotation it is inextricably linked to the record for as long as the record exists. It should contain all the elements of intellectual form necessary to identify uniquely a record and place it in relation to other records belonging in the same aggregation. Thus, it should represent the conceptual place where the administrative-documentary procedure joins with intellectual form, and where all components of intellectual form converge together. In fact, depending on whether a record is made or received, it should include most of the following elements: register number (if applicable), date of record, date and time of receipt, date and time of transmission (either across space or across time, that is, to the system itself), state of transmission (i.e., whether the record is a draft, an original, or a copy), mode and medium of transmission, archival date (i.e., the date on which the record becomes part of a dossier or class), register number of sending office (if applicable), names and addresses of creator, originator, author, writer, addressee, and any other recipient, action or matter, attachments, security protection type and means, information configuration, medium, type of file (e.g., WP, MS, Excel, Mime encoded), handling office, action taken, class code, dossier identifier (if applicable), record item identifier, and other elements required by the specific creator or activity. In electronic records systems designed to produce a record profile annotation for each record sent or closed, most of the fields listed above would be directly filled by the system itself on the basis of (1) the record header, (2) the electronic space in which the document is made or received, (3) the competence¹⁷ of the person writing the document, as reflected in the access privileges,¹⁸ and (4) the document to which the one being made replies, etc. A few fields would be filled by the author and the records office. On the basis of the findings of the UBC-MAS research, there is no doubt that, in time, the record profile will fulfill for electronic records the same function that the protocol and the eschatocol accomplish for traditional textual records.

With regard to the **persons** concurring in the production of electronic records, the requirement for atomic control presented by this type of record imposes a multiplication of the persons of which a diplomatist/archivist needs to keep track. Diplomats says that, while many persons may take part in the creation of a record (among them, witnesses and countersigners), only three persons are necessary to its existence, that is, the *author* (i.e., the person having the authority and capacity to issue the record or in whose name or by whose command the record has been issued),

the *addressee* (i.e., the person to whom the record is directed or for whom the record is intended), and the *writer* (i.e., the person having the authority and capacity to articulate the content of the record).

However, the integration of the components of traditional records is such that, once the author, addressee, and writer are identified, the creator and the originator are obvious. It is not so with electronic records. *Creator* and *originator* need to be identified for each electronic record made or received and set aside for action or reference, the creator being the person producing the archival fonds in which the record in question belongs, and the originator being the person owning the electronic address or space in which the record has been generated (i.e., from which the record is transmitted or in which the record is compiled and closed).

The primary reason for the identification of the creator in connection with each electronic record relates to preservation over time. In fact, while the records are in the live electronic system in which they are produced, their creator is easily identifiable as the person having jurisdiction over the system for making, receiving, and accumulating records in the conduct of business. But, once the records are taken out of the system, their location on a storage medium and in a given storage facility is no longer meaningful for the purpose of identifying their creator. In an ideal system, the identity of the creator of an electronic record would be revealed by a visual or presentation component of the record profile form attached as an annotation to each record item, such as a logo or a crest.

The primary reason for the identification of the originator in connection with each electronic record is that such persons may be different from the author or writer of the record, especially when a record has multiple authors but only one of them is responsible for its transmission: the issue relates primarily to responsibility and accountability. The identity of the originator of a record electronically transmitted is in the header of the mail message, while that of the originator of a record that has not crossed electronic boundaries is included by the system in the record profile and corresponds to the name of the owner of the electronic individual space in which the record is closed.

The **action** is the core component of every record, regardless of its medium and form. An action is any exercise of will which aims to create, change, maintain, or extinguish situations. A special type of action is a *transaction*, which is an action between two or more persons, aiming to change the relationship existing between them. The relationship between an electronic record and the action in which it takes part is usually revealed by the conceptual position that the record occupies in the dossier or the class of records to which it is connected by a classification code. Such relationships may be similar in nature to the relationship that traditional records have with juridical acts: *dispositive* (when the record is the essence of the act, which comes into existence with the creation of the record, e.g., the electronic records admitting patients to a hospital), or *probative* (when the record is proof of an act which is complete before the creation of the record, e.g., the electronic lists of registered voters).

However, most electronic records have a *supporting* function with respect to the action in which they take part. For example, a geographical informational system, that is, a relational database which presents data in a geographic arrangement, contains

only documents (i.e., information affixed to a medium in an objectified and organized way, according to specific rules of representation), information (i.e., a meaningful group of data intended for communication, either across space or through time), or individual data (i.e., the smallest meaningful recorded facts). However, it can itself be considered a record, if its function as a database is to support a specific business activity (it does have all the necessary components of a record when it is regarded as a unit), and can produce documents that, once extracted from it and linked to other records of action, become records (e.g., a representation of the intensity of traffic in a given place that is attached or linked to a report containing recommendations for the regulation of city traffic). Another large portion of electronic records has a *narrative* function, that is, it does not relate to business activity other than by being the expression of the way in which individuals set themselves to work and go through the informal motions of carrying out activities and decision making. While they are records themselves, they are not procedurally bound to action in the way in which the other types of records are, but relate to it in an indirect way. Supporting and narrative records are records whose existence is not required by the juridical system, but that are generated by their author for his or her convenience and by choice.

Context refers to the juridical-administrative framework in which the action takes place. With electronic records it is essential not to confuse the technology context with the administrative one. For example, there is no such thing as “shared electronic records.” While there can be “shared databases,” which contain documents, information, or data accessible to many persons, each database is the responsibility of only one juridical person (and this can be a consortium of persons), and each person who uses documents, information, or data contained in a shared database in the course of its own activity generates with them in its own electronic system its own electronic records. The other point to be made in this regard is that electronic records are not generated every time a database is queried, but only when this is done in the context of a business action and both the query and the reply become part of the records of such action; in other words, most electronic “transactions” are not related to business actions and do not generate records. Ultimately, the key to the existence of an electronic record is the **archival bond**.

The archival bond, which refers to the link that every record has with the previous and subsequent one in the conceptual net of relationships among the records produced in the course of the same activity, is an essential component of the record, in keeping with our understanding that records are necessarily composed of documents and the complex of their relationships. It is originary (i.e., it comes into existence when the record is made or received), necessary (i.e., it exists for every record), and determined (i.e., it is characterized by the purpose of the record).¹⁹ With traditional records, this bond is implicit in the records’ physical arrangement. With electronic records, it is necessary to make it explicit. The formation of the archival bond—which conceptually arises at the moment a record is set aside, and in so doing determines the moment of the record’s creation—may be manifested in the specific classification code assigned to the record, which connects it to other records belonging to the same class, or, in the case of incoming and outgoing records, in the registration number assigned to the record, which connects it to previous and subsequent records made or received by the creator and dealing with the same matter.²⁰

In a sophisticated electronic system, both annotations would be included in the record profile, thereby fixing the record's relations and stabilizing them at the point of the record's incorporation into the central record system. In systems that are not designed specifically for keeping records, classification code or filing identifier and, if applicable, registration number are part of the metadata which constitute the data dictionary.

Content refers to the message the record is intended to convey. The content of an electronic record, for the record to exist at all, must be fixed and stable. This implies that so-called "virtual documents" cannot be considered records in the electronic environment. A virtual document consists of pointers to data residing in different locations within a database, or in multiple databases. While it is possible to see on a computer monitor the document resulting from the assembly of those data in a meaningful form, this document does not exist as such until its components are actually joined together in an inextricable way, that is, until the content of the document is explicitly articulated in a fixed form. This is different from what happens with traditional records, where a document constituted of pointers to information contained in other documentary sources is a record of the sources to be used to make another record. With electronic documents, the pointers lead to data which—being contained in databases that, by their nature, are dynamic—may vary over time. Thus, a virtual document lacks stability and may be ten different documents in a ten minute time span.

The characteristics of electronic records as articulated by diplomatics and archival science constitute the conceptual basis for establishing first, whether the electronic system we are confronted with contains records, and second, whether these records can be considered reliable and authentic. As it regards the second issue, it is necessary to specify what is intended by reliability and authenticity.²¹

Reliability refers to the authority and trustworthiness of records as evidence, that is, their ability to stand for the facts they are about. Reliability depends upon two factors: the degree of completeness of the record's form and the degree of control exercised over its procedure of creation. The *completeness* of the form of the record refers to the fact that the record possesses all the elements of intellectual form necessary for it to be capable of generating consequences. Traditionally, no record can be considered complete if it does not contain in its intellectual form the date (which expresses the relationship between the record and its author, and between the fact observed in the record and its observer), and the signature (which assigns responsibility for the record and its content, and makes of the record a fact to be observed). With electronic records, the date given to the record by its author is not sufficient to make a record complete: the date and time of transmission to either an external or internal addressee, or the date and time of transmission to the dossier or class in which the record belongs is necessary. Moreover, the signature, whether typed or handwritten, cannot fulfill its traditional function because it can be attached to the record by anyone without the possibility of verifying its authenticity, thus it does not contribute to the record's completeness. With electronic records, the function of the signature is accomplished either by the name contained in the header of mail messages or in the profile of other record types and/or by electronic seals or so-called "digital signatures," which do not have the form of signatures at all.

Procedure of creation refers to the body of rules governing the making, receiving, and setting aside of records:

Some of these rules refer to record-makers, by establishing who is competent for signing what records, by giving responsibility to different persons for recording the same facts, or by requiring that the same fact or part of it be reported at the same time to different addressees. Other rules refer to the routing of the records, their handling in the course of their compilation and completion, and their filing, as this operation determines the record's documentary context. The more rigorous and detailed the rules, the more established the routine, the more reliable the records resulting from their application will be.²²

In electronic systems, there are two kinds of methods for ensuring that these rules are respected and that the reliability of record makers is ensured. The first kind is directed toward prevention, and includes three main methods. One method consists of embedding within the system access privileges, that is, of assigning to each person who has access to the electronic system, on the basis of his or her specific competence, the authority to compile, classify, annotate, read, retrieve, transfer, and/or destroy only specific groups of records (these privileges might connect each person to classes or sub-classes of records, or to types of records). A second method consists of embedding in the system "workflow rules" according to which the system will present the person competent for each action—and only this person—with the related records—and only with those records—and will solicit the making of the appropriate record at the proper time in the automatic development of the procedure. A third method consists of limiting physical access to the technology or to parts of it by means of magnetic cards, passwords, fingerprints, etc.

The other kind is directed toward verification and includes one primary method. It consists of designing within the electronic system an "audit trail," that is, the automatic recording of all interactions with records, so that any access to the system can be documented as it occurs, be it a modification made to a record, a deletion, an addition, or a simple viewing of a record. Other rules governing the making, receiving, and setting aside of records refer to their routing,²³ their handling in the course of compilation and completion, and their filing, as this operation determines the record's archival bond. These recordkeeping rules tend to be procedural in nature, and thus external to the electronic system; they also govern all the records of the same creator, that is, they apply to both electronic and non-electronic records.

Control over the record-creation process is strengthened even further by the integration of these recordkeeping rules with specific business processes. Integrating business and documentary procedures includes: identifying all the business procedures within each agency function; breaking each procedure down into its standard six phases (initiative, inquiry, consultation, deliberation, deliberation control, execution);²⁴ and determining, for each phase, the act being carried out, the intellectual form of the record generated, the office competent to generate it, its classification, its level of confidentiality, the means of authenticating it, its need for auditing, and its disposition. The integration of business and documentary procedures results in a description of

the records associated with each phase of each procedure and the specific requirements linked to them in relation to access privileges, classification, registration, authentication, auditing, and so on.

Reliability and the methods for guaranteeing it are linked exclusively to records creation.²⁵ **Authenticity**, on the other hand, is linked to the record's mode, form, and state of transmission, and to the manner of its preservation and custody, and is protected and guaranteed through the adoption of methods that ensure that the record is not manipulated, altered, or otherwise falsified after its creation, that is, the record is precisely as reliable as it was when made, received, and set aside. The *mode of transmission* of a record is the method by which a record is communicated over space or time. The more secure the method of transmission, the higher the guarantee that the record received is what it purports to be. The *form of transmission* of a record is the physical and intellectual form that the record has when it is received. Traditionally, authenticity is best ensured by guaranteeing that a record maintains the same form through transmission, both across space and through time.

In relation to transmission, however, the main difference between traditional and electronic records relates to the state of transmission. The *state of transmission* of a record refers to its degree of development and authority, that is, its primitiveness, completeness, and effectiveness when it is initially set aside after being made or received. This state can be either draft, original, or copy. A *draft* is a temporary compilation of a document intended for correction; drafts may be in various stages of completion. A *copy* is a reproduction of a record made either from an original, a draft, or another copy. An *original* is the first complete and effective record. In other words, in order to be original, a record must present three characteristics: completeness (i.e., its form must be the one intended by its author and/or required by the juridical system), primitiveness (i.e., it must be the first to be produced in its complete form), and effectiveness (i.e., it must be capable of reaching the effects for which it was produced). With electronic records, the state of transmission is assessed in relation to their routing. Any record that is neither transmitted to an addressee nor consigned to the dossier or class to which the record belongs within the central records system (i.e., the archives or archival fonds of the creator), but that is saved in the electronic space in which it is made, is to be considered a draft because it is incomplete: in fact, the act of transmitting a record across either external or internal electronic boundaries necessarily adds components to the record which makes it complete (among these, the date of transmission and the "superscription," that is, the identity of the originator and/or author). Any record that is transmitted is received as an original, but it is saved in the space of the originator as a final draft, because, although the system will add to it the time of transmission and the identity of the originator, this record is not capable of reaching its purpose and lacks effectiveness (the system saves to the space of the originator—the individual space—a copy of every record transmitted, even if this, for whatever reason, never reaches the intended address). Every time a person retrieves a record from the central records system, he or she has a view of the original—in the case of a record received or an internal record—or of the last draft—in the case of a record sent. If the person copies the record to his or her own space, the result is an imitative copy rather than a copy in the form of original, because some of the metadata, or of the data about the record contained either in the record profile or elsewhere in the system, change. Every time a person forwards a record to another

person, he or she creates an insert of the type of a *vidimus*, and so on. The basic concept is that, with electronic records, the state of transmission is assessed on the basis of the way in which electronic transmission affects the form of the records, every aspect of it, including the annotations (e.g., the data included in the profile or the data included in the data directory and the data dictionary).

In relation to preservation and custody, the main difference between electronic records and traditional records is that the latter are kept authentic by maintaining them in the same form and state of transmission in which they were when made or received and set aside, while the former are kept authentic by continuous copying and periodic migration. Thus, no electronic record will ever survive for more than a decade in its original form (the term “survival” does not refer exclusively to physical existence, but includes readability and intelligibility). The authenticity of electronic records in the long term can only be ensured by self-authenticating processes of reproduction from one medium to another and of conversion from one digital technology to another; by the reliability of the person or office entrusted with the authority and the capacity of carrying out the reproduction²⁶ and conversion processes; and by an uninterrupted line of physical custody.

The processes need to be approved, validated, and periodically audited by a higher authority external to the records creator, and the person or office responsible for their accomplishment must be invested with the ongoing competence for those processes by the same controlling authority (moreover, as mentioned earlier, such a person or office must be a neutral third party). As to custody, now more than ever it shall be the exclusive competence of professional archivists, for three reasons: (1) because record creators are accountable *for their action* through their records, while it is archivists who are accountable *for the records* themselves; (2) because record creators have the right to demonstrate that they have carried out their responsibilities (i.e., they have the right to be considered discharged of their duties, or to prove that they have discharged their duties) by putting the records of their activities in the hands of a third party; and (3) because—no matter how carefully the processes of reproduction and conversion have been carried out, and no matter how much authority and responsibility are given to those invested with the supervision of those processes—the verification of the authenticity of electronic records over the long term will have to rely on one thing and one thing only: their *archival description*.

When the electronic records that researchers wish to use as sources have gone through several reproductions and conversions, when their physical form has lost most of its original features, when their creators and the persons competent for copying and migrating them are defunct and thus unable to vouch for their trustworthiness, the ultimate instrument for assessing their authority will be the archival inventory. The intellectual arrangement and the description of archival fonds serve a critical authenticating function for inactive records by preserving and perpetuating their network of administrative and documentary relationships—in other words, their context and their archival bond. Administrative relationships are revealed and preserved through the writing of the administrative history of the archival fonds and its parts, including its preservation and custodial history. Documentary relationships are revealed and preserved through the identification of the levels of arrangement of the fonds and their representation in structured descriptions. With electronic records,

a description of the general operating system and its architecture, of the records architecture, and of the metadata as they have changed over time will need to be added.

The main conceptual findings that emerge from the analysis described above may be divided into two categories: (1) specific methods for ensuring the reliability and authenticity of electronic records and (2) broader management issues concerning the maintenance²⁷ and preservation of reliable and authentic records.

Regarding methods for ensuring the reliability and authenticity of electronic records, the major findings may be summarized as follows:

1.(i) The reliability and authenticity of electronic records are best ensured by embedding procedural rules in the overall records system²⁸ and by integrating business and documentary procedures.

The rules embedded within the records system establish agency-wide control over the creation, handling, and preservation of records, both electronic and non-electronic, while the integration of business procedures and documentary procedures strengthens this control, by embedding it within specific business processes.

1.(ii) The reliability and authenticity of electronic records are best guaranteed by instituting procedures that tighten and strengthen the archival bond, such as classification, registration, and profiling.

The research project's emphasis on the record's documentary context derives from its assumption that to ensure the reliability of records it is necessary to fix their relations. This need to stabilize records by fixing their relations, however, must be balanced with the equally important need to respect the natural dynamism of the records system. By focussing on the archival bond, which provides the connective tissue between individual records, and on the documentary context arising from that original bond, which provides the connective tissue among all the records, it is possible to exercise a considerable degree of control over the creation and handling of records without impeding the natural dynamism of the records system or imposing unreasonable requirements upon it.

1.(iii) The reliability and authenticity of electronic records can only be preserved if the management of the electronic and non-electronic components of the records system is integrated.

This integration is accomplished by instituting procedures for creating an electronic record profile for every non-electronic record that is consigned to the central records system as well as for every electronic record that is set aside, and by establishing a repository of those record profiles. The idea behind the electronic repository is to allow users of the records system a complete view of all the profiles of the records belonging to the same dossier or class, regardless of their media. When a matter is concluded and the dossier is closed and removed from the central records system, along with its profile, the repository would continue to maintain a final view of the profiles of all the records in the dossier. This final view serves the purpose of authenticating the dossier at the point at which it leaves the central records system for low cost storage, and preserving a trace of all actions if the dossier is destined for destruction.

Regarding broader management issues relevant to the maintenance and preservation of reliable and authentic records, the major findings are as follows:

2.(i) The life cycle of the managerial activity directed to the preservation of the integrity of electronic records may be divided into two phases: one aimed at the control of the creation of reliable records and to the maintenance of authentic active and semi-active records, and the other aimed at the preservation of authentic inactive records.

The separation of the managerial activity into two phases is based on the research team's finding that the intellectual methods necessary for guaranteeing the integrity of electronic records while they are needed by the body which produced them are different from the intellectual methods necessary for ensuring their integrity when they are needed by society for purposes other and broader than the ones for which they were created. While records are being produced and used by the record creator, their reliability is ensured by procedural and technological methods aimed at the control of the trustworthiness of their authors and of their creation process and at the definition of their forms, and their authenticity is guaranteed by the adoption of procedural and technological methods aimed at ensuring their proper identification in context (administrative and documentary), and their secure transmission and maintenance. When the records are no longer needed by the body which produced them, however, their authenticity must be protected by physically transferring them to an archival institution or programme and, once transferred, by arranging and describing them.

2.(ii) Once records become inactive, the perspective on them shifts from a bottom-up perspective to a top-down one.

The control of record creation, completeness, and handling through means such as procedure and form design, classification, scheduling and registration, and retrieval of active records, and the control of record preservation through means such as procedures for removal, storage, and review, profile management, and copying and conversion of semi-active records, reflect a bottom-up perspective on the record, one which begins from the record as an individual entity—with its characteristics, attributes, and relationships in the course of formation and development—and then proceeds toward the first level of aggregation (e.g., the dossier), without ever reaching the level of series. On the contrary, the selection, arrangement and description, and preservation and retrieval of inactive records reflect a top-down perspective, one which begins with the fonds and then proceeds to examine its already stabilized components, the series, and their parts.²⁹ It is not coincidental that, when records are in the phases of formation and sedimentation, they are seen to accumulate within classes, while, when they are no longer susceptible of change and accretion, they are seen as belonging to series: a class is an intellectual container to which records are individually assigned as they are made or received and set aside, while a series is a concrete body of records, which exists as a whole before revealing itself as a sum of parts. This shift in perspective necessarily implies a shift in responsibility for protecting the record's reliability and authenticity from the record creator to the record preserver.

2.(iii) The integrity of electronic records is best preserved by entrusting the creating body with primary responsibility for their reliability and authenticity while they are needed for business purposes, and the preserving body with responsibility for their authenticity over the long term.

While records are being used in the course of and for reasons of the usual and ordinary conduct of business, an agency has a direct interest in making and maintaining reliable and authentic records in order to carry out its activities. Once the records are no longer used and relied upon in the course of business, however, the circumstantial guarantee of trustworthiness that the agency's reliance on the record provides cannot be assumed any longer.³⁰ So the question is: How do we protect the authenticity of records after the business in which they actively participated is concluded and the creator does not need to rely on them anymore, especially when we consider that the continuing reliance of the organization on the record is a way of authenticating it? The research team's findings suggest that the routine transfer of records to a neutral third party, that is, to a competent archival body, invested with the exclusive authority and capacity for the indefinite preservation of inactive records, is an essential requirement for ensuring their authenticity over time. The competent archival body would assume the form of an autonomous office or programme within the agency if the creating agency maintains its own historical archives, or a separate agency if the creating agency routinely transfers its records to an archival institution.³¹

The need for a two-phase life cycle approach to the management of records in both electronic and non-electronic form, and the fact that responsibility for managing those records must necessarily shift from the record creator to the record preserver when the records reach the inactive phase, challenge the adequacy of the life continuum approach as an appropriate managerial model for corporate records in either electronic or non-electronic form. The life continuum approach was articulated in the 1980s in Canada as a reaction to the separation of records management and archival functions that had derived from the North American adaptation of the traditional life cycle approach, and was intended to promote the overlap and integration of those functions.³² The traditional life cycle approach separated the management of records into two distinct phases, with the records manager assuming responsibility for the first phase (i.e., the "records" phase), and the archivist assuming responsibility for the second phase (i.e., the "archives" phase). In contrast, the continuum approach proposed to integrate and unify the management of records. The advantage of the continuum approach is that it has determined the rejection of the Schellenbergian notion of records and archives as two distinct entities possessing different natures and it has forced archivists to think more seriously about means by which records can be better controlled from the point of their creation.

However, the continuum approach has fostered at best an integration and at worst a confusion of responsibility, accountability, and jurisdiction for records that fails to recognize very real differences in the maintenance of active, semi-active, and inactive records, differences that are more, rather than less, significant in an electronic environment. For example, in one of his interpretations of the continuum model, David Bearman writes: "The records continuum...can help reunify recordkeeping around its proper focus, the documented event...as it...places the issue of control of the record from the moment of its creation within the context of the event that gave

rise to the record and the organisation or person whose activity it documents.”³³ Such item level control from the point of a record’s creation “obviates the need to accession, arrange, process, and describe records after ‘transfer’, or even to take custody.”³⁴ This interpretation ignores four fundamental issues relevant to the management of records over time. Firstly, the archival bond, which is an essential component of the record, changes and develops until the record reaches the point of stability, that is, until the action to which it relates is concluded. This implies that the entity record is in formation during its period of activity, as the aggregations in which the record belongs are constantly accruing and changing, according to the natural dynamism of the records system. When the records become semi-active, their documentary context is subject to development and change as only some components of each class will be removed from the records system and accumulated together to build up series. When the records become inactive, the archival bond is defined and stabilized and not subject to further changes. This is the situation that needs to be preserved over the long term. Thus, in a very real way, the record creator is responsible for an entity (the record) in the course of development, while the record preserver is responsible for an entity (the same record) completely developed.

Secondly, the “descriptions” of the records generated by the record creator—“metadata” in electronic systems—have the purpose of identifying the records in the atomic context of the activities in which they participate and of the uses made of them, and are themselves records of the data that the creator needs about its own records. Being contemporary to the records, such “descriptions” put into being and manifest the archival bond at the item level, and come into existence for all the records created. On the contrary, the descriptions of the records that are made by the archival preserver come into existence only for the records that have survived after their administrative usefulness to the creator has been exhausted, and are meant to identify the records as historical aggregations (i.e., formed over time) in their evolving administrative and documentary context, and to show the record aggregations as they present themselves once their internal relationships are stabilized. Metadata may well obviate the need for description below the series level but it does not obviate the need for description at the series level and higher.³⁵

Thirdly, the selection of the records—particularly of electronic records—is carried out at the item level when the records are in formation, driven only by the specific action and information needs of the person handling an affair; then it is carried out at the dossier level once the affair in question is concluded, according to a predisposed timetable built on the basis of the needs and requirements of the creator and in the context of the specific activity to which the dossiers relate. On the contrary, when the records become inactive, they are selected in a much broader context, which often goes beyond that of the creator, and takes into account more general and long term purposes.

Finally, the accessibility of records within the jurisdiction of the creator is exclusively on the basis of the competence and need to know for action purposes of the person requiring access, while the dissemination of inactive records is mostly for purposes different from those generating them.

All the above aims only to point out that, while activities conducted on records during their active, semi-active, and inactive periods may be called by the same name, such as maintenance, description, selection, and dissemination, they are fundamentally and substantially different, besides being different as to perspective. This is the more so with electronic records, whose different attributes in the various periods of their life cycle are not so clearly visible and recognizable and need therefore a proactive effort of identification. However, the statements above should not be taken to imply that archivists should not have a say in the first part of the life cycle. On the contrary, this research has demonstrated that the knowledge which belongs to and identifies the professional archivist, and is constituted by diplomatics and archival science, is indispensable to the design of records systems and recordkeeping and preservation systems capable of serving the business and accountability needs of a record creator so that its records will be created reliable and maintained authentic as long as they are needed for action or reference. By the same token, the knowledge that the creator has of its own records is essential to the archivist who needs to plan a migration platform for them. But, ultimately, different parties are and should be accountable for different functions: the creator should be accountable for its action *through its records*, the preserver should be accountable *for those records*. This division of responsibility is what ensures the authenticity of inactive records and makes of them the impartial sources that society needs.

The questions the UBC-MAS project raises about the adequacy of the continuum concept as the intellectual basis for developing means of protecting the integrity of inactive records are not insignificant when one considers the centrality of such a concept to contemporary approaches to the management of electronic records. It is, for example, at the heart of the recently-completed "Recordkeeping Functional Requirements Project" at the University of Pittsburgh. The Pittsburgh Project was a three-year National Historical Publications and Records Commission (NHPRC)-funded research project, the purpose of which was "to develop and test recordkeeping functional requirements and their applicability in electronic recordkeeping systems."³⁶ Although the Pittsburgh Project and the UBC-MAS project have similar aims, their perspectives are fundamentally different. The Pittsburgh Project's identification of functional requirements reflects the continuum perspective. The requirements do not differentiate the needs of active and semi-active records from the needs of inactive records, and they are based on the premiss of a complete integration of responsibility, accountability, and jurisdiction for the management of electronic records. The UBC-MAS research project's identification of recordkeeping requirements (based on an analysis of the activities involved in creating, handling, and preserving electronic records) reflects a life cycle perspective. The requirements here focus on the needs of active and semi-active electronic records and they are based on the premise of an essential division of responsibility, accountability, and jurisdiction at the point at which those records become inactive.

The different perspectives taken in the two projects are undoubtedly a consequence of the different methods³⁷ and assumptions adopted by each. The Pittsburgh Project's recordkeeping requirements are justified and validated on the basis of practical standards and practices that have developed within a particular juridical context.³⁸

The recordkeeping requirements identified in the UBC-MAS project, on the other hand, are justified and validated on the basis of universal standards and practices drawn from the theory and methodology of diplomatics and archival science.

The difference in methods is also reflected in the way in which concepts have been defined and terminology chosen and used. The meaning of key terms can be defined in one of two ways. It can be defined for the purpose of the project at hand (writers of legislation, for example, often adopt this approach), or it can be taken directly from the traditional use and understanding existing in the context of the body of knowledge in which the terms have been developed. While the Pittsburgh Project has chosen the former approach, the theoretical choice made by the UBC-MAS project has imposed the latter approach. As a consequence, fundamental concepts, such as *record*, are defined by each project in substantial different ways.³⁹

The differences are not only of definition, but also of interpretation. The expression “functional requirement,” for example, has been attributed a specific meaning by the Pittsburgh Project which is different from the one generally accepted and understood by computer science.⁴⁰ In the Pittsburgh Project, functional requirements consist of broad, generic standards for recordkeeping which are not directly translatable into system design requirements. In the UBC-MAS project, the meaning of a functional requirement is the computer science meaning. The requirements consist of specific rules for each activity associated with creating, handling, and preserving records which are capable of direct implementation by system designers. In the Pittsburgh Project, the identification of functional requirements constituted the researchers’ starting point; in the UBC-MAS project, it constitutes the final outcome of the research.

Although their differences are fundamental and, likely, irreconcilable, given the radically different perspectives, methods, and assumptions on which they are based, the two projects share a common purpose: ensuring the integrity of electronic records. Implementation of the two models in a variety of organizational settings will demonstrate which approach offers the most effective means of achieving that purpose.

As a consequence of its findings concerning the necessity of adopting a two-phase life cycle approach to the management of electronic records, the same research team at UBC is now in the process of proposing another research project that will assume the point of view of the record preserver. Its overarching goal will be to identify, on the basis of diplomatic theory and archival science, a comprehensive methodology, applicable across juridical systems, cultures, and technologies, for preserving the integrity of electronic records from the moment when they are no longer needed by the body producing them and for as long as they are needed by society at large. Its specific objectives are:

1. To formulate, from a purely conceptual point of view, appraisal strategies for electronic records, including the timing and form of a reliable transfer of responsibility for their preservation from the body producing them to an archival institution or programme;
2. To establish the physical form of preservation that will guarantee the continuing reliability and authenticity of electronic records;

3. To articulate environmental and media standards for the preservation of authentic electronic records;
4. To determine the principles guiding the institutional articulation of reliable and self-authenticating procedural methods for overcoming media and digital obsolescence;
5. To identify appropriate intellectual methods for ensuring the continuing accessibility and retrievability of electronic records;
6. To develop criteria for description of electronic records that is capable of communicating their nature and characteristics to scholars and the general public; and
7. To assess existing methods and standards for the implementation of access and privacy legislation in relation to electronic records, and, if necessary, develop new ones.

The proposed research project is envisaged as an international collaboration among Canadian, American, and European archivists in recognition of the fact that the methods of long-term preservation must be applicable across juridical systems, cultures, and technologies and must constitute the foundation of international standards.⁴¹

The UBC-MAS research project was undertaken to test the validity of traditional diplomatic and archival concepts in the brave new world of electronic records. The conceptual analysis of electronic records and the project's findings confirm that the concepts continue to have resonance and, in fact, provide a powerful and internally consistent methodology for preserving the integrity of electronic records. At the same time, situating the analysis within a knowledge engineering framework has resulted in a fruitful re-examination and adaptation of diplomatic and archival concepts in light of the electronic records reality and helped to breathe new life into archival theory, methodology, and practice.

Notes

- 1 The UBC research team comprises Luciana Duranti as principal investigator, Terry Eastwood as co-investigator, and Heather MacNeil as research assistant.
- 2 Luciana Duranti and Terry Eastwood, "Protecting Electronic Evidence: A Progress Report," *Archivi & Computer* 5, no. 3 (1995), p. 214, hereafter *First Progress Report*.
- 3 *Ibid.*, p. 215.
- 4 Progress reports have been issued by members of the research team at various stages in the project. See Duranti and Esatwood, "First Progress Report," pp. 213-50; Luciana Duranti, Heather MacNeil, and William E. Underwood, "Protecting Electronic Evidence: A Second Progress Report on a Research Study and Its Methodology," *Archivi & Computer* 6, no. 1 (1996), pp. 37-70; Luciana Duranti and Heather MacNeil, "Protecting Electronic Evidence: A Third Progress Report on a Research Study and Its Methodology," *Archivi & Computer* 6, no. 5 (1996, forthcoming).
- 5 "First Progress Report," pp. 214-15.
- 6 Term definitions and templates are included in *Ibid.*, pp. 213-33.
- 7 Although valid for managing non-corporate (i.e., personal) fonds, the model would have to be much more simplified because considerations of administrative and public accountability do not impinge on individuals in the same way they impinge on corporate bodies. For example, the reliability and authenticity

- of a record created by a private person will be determined in relation to its form, not its procedure of creation or its transmission. Such authenticity will only be tested when the individual record is presented for some specific purpose.
- 8 The activity and entity models, the glossary, and the rules associated with the activities are available for viewing at the UBC-MAS Research Project home page at <http://www.slais.ubc.ca/users/duranti>.
 - 9 Semi-active records fall within the purview of both the recordkeeping system and the record-preservation system. The recordkeeping system is concerned with semi-active records as they relate to active records and the carrying out of the actions for which the records were created. The record-preservation system, on the other hand, is concerned more generally with locating, retrieving, and preserving semi-active records for the creator's reference purposes.
 - 10 An authentic copy is "a copy certified by officials authorized to execute such a function, so as to render it legally admissible as evidence." See Luciana Duranti, "Diplomatics: New Uses for an Old Science," *Archivaria* 28 (Summer 1989), p. 21.
 - 11 An imitative copy "reproduces, completely or partially, not only the content but also the forms, including the external ones (layout, script, special signs, medium and so on), of the original [record]." See *Ibid.*, pp. 20-21.
 - 12 A simple copy "is constituted by the mere transcription of the content of the original." A *vidimus* falls within the category of an authentic copy and takes the form of an insert, i.e., a document "entirely quoted (if textual) or reported (if visual, like maps) in subsequent original documents in order to renew [its] effects. ...An authentic copy in general and a *vidimus* in particular, only guarantees the conformity of the copy to the original text." See *Ibid.*, pp. 21, 26 (endnotes 38 and 39).
 - 13 The superscription is "the mention of the name of the author of the document and/or the action. See Luciana Duranti, "Diplomatics: New Uses for an Old Science (Part V)," *Archivaria* 32 (Summer 1991), p. 12.
 - 14 The inscription is the mention of "the name, title and address of the addressee of the document and/or action." See *Ibid.*, p. 12.
 - 15 The protocol is the first of three physical subsections of a document. It "contains the administrative context of the action (i.e., indication of the persons involved, time and place, and subject) and initial formulae." See *Ibid.*, p. 11.
 - 16 The eschatocol is the last of three physical subsections of a document. It "contains the documentation context of the action (i.e., enunciation of the means of validation, indication of the responsibilities for documentation of the act) and the final formulae." See *Ibid.*, p. 11.
 - 17 Competence is a sphere of functional responsibility entrusted to an office or officer.
 - 18 Access privileges refer to the authority to compile, classify, annotate, read, retrieve, transfer, and destroy records, granted to others within an agency.
 - 19 Giorgio Cencetti, "Il fondamento teorico della dottrina archivistica," *Archivi* II, VI (1939), p. 8, reprinted in Giorgio Cencetti, *Scritti archivistici* (Rome, 1970), p. 39. Jenkins uses the term "interrelatedness." See Hilary Jenkinson, "Introductory," in Public Record Office, *Guide to the Public Records, Part I* (London, 1949), p. 2.
 - 20 In many European countries, the registration of incoming and outgoing records in a register has, for centuries, ensured reliability by tracking all the records sent and received by an agency and, within that scope, mapping all the actions associated with a matter and the way it was disposed. In the UBC-MAS project, the establishment of registration procedures, which include maintaining an electronic protocol register, has been identified as one of the rules of the recordkeeping system. As an instrument of documentary control, the protocol register is designed to serve both records management and accountability purposes. At the same time, it is a valuable instrument for capturing documentary context, since it reflects the relations among all the records that have entered and exited the agency.
 - 21 For a more detailed discussion of these concepts, see Luciana Duranti, "Reliability and Authenticity: The Concepts and Their Implications," *Archivaria* 39 (Spring 1995), pp. 5-10.
 - 22 *Ibid.*, p. 6.
 - 23 The routing of electronic records involves establishing the boundaries of general, group, and individual space within the electronic system by defining in which of these spaces records may be made, received, registered, classified, revised, stored, and so on.
 - 24 See Luciana Duranti, "Diplomatics: New Uses For An Old Science (Part IV)," *Archivaria* 31 (Winter 1990-91), pp. 14-19.

- 25 Reliability, it should be pointed out, is also a matter of degree. The methods identified by the UBC-MAS research team are designed to achieve the maximum degree of reliability. Individual record creators will have to determine for themselves the degree of reliability required for each type of record created, depending on the business purposes the record serves and the legal requirements associated with it. The methods described here will be, necessarily, selectively applied.
- 26 This is of course a responsibility involving supervision over and accountability for the technical work.
- 27 The detailed rules developed by the project may be found on the World Wide Web home page of the project and in the third and fourth progress reports on the project published in *Archivi & Computer* 6, nos. 2 and 7.
- 28 The records system and its components are defined earlier in this article. See pp. 46-57, *supra*.
- 29 For a more detailed discussion of the research project's findings as they relate to the top-down perspective of archival description, see Heather MacNeil, "Implications of the UBC Research Results for Archival Description in General and the *Rules for Archival Description* in Particular," *Archivi & Computer* 6, nos. 3-4 (1996), pp. 239-46.
- 30 Protecting authenticity may even run counter to narrowly-defined agency interests. A recent example is the alleged tampering and destruction of documents by the Department of National Defence relating to the 1993 torture death of a Somali at the hands of members of the Canadian Armed Forces in Somalia.
- 31 For a detailed discussion of the significance of archival custody to the authentication of records over time, see Luciana Duranti, "Archives as a Place," *Archives and Manuscripts* 24, no. 2 (November 1996), pp. 242-56 and Terry Eastwood, "Should Creating Agencies Keep Electronic Records Indefinitely," *Ibid.*, pp. 268-85.
- 32 The main features of the continuum approach as it has developed in North America are outlined in Jay Atherton, "From Life Cycle to Continuum: Some Thoughts on the Records Management-Archives Relationship," *Archivaria* 21 (Winter 1985-86), pp. 43-51.
- 33 David Bearman, "Item Level Control and Electronic Recordkeeping," paper delivered to the annual meeting of the Society of American Archivists, San Diego, California (29 August 1996), p. 23.
- 34 *Ibid.*, p. 22.
- 35 For a more detailed discussion of the relationship between metadata and archival description, see Heather MacNeil, "Metadata Strategies and Archival Description: Comparing Apples to Oranges," *Archivaria* 39 (Spring 1995), pp. 22-32.
- 36 Richard J. Cox, "Putting the Puzzle Together: The Recordkeeping Functional Requirements Project at the University of Pittsburgh; A Second Progress Report," in *University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers: Progress Report Two* (Pittsburgh, March 1995), p. 1.
- 37 The methods adopted by the Pittsburgh research team have been discussed by Seamus Ross in his "Commentary on the Pittsburgh University Recordkeeping Requirements Project: A Progress Report (Delivery Draft)," a paper presented at the Society of American Archivists' Annual Meeting in Washington, D.C. (September 1995).
- 38 The functional requirements are justified on the basis of "cultural warrant" and validated on the basis of case studies of "organizational culture." The investigations of both cultural warrant and organizational culture focus exclusively on American recordkeeping practices and requirements. See Richard J. Cox, ed., "University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers," (Pittsburgh, September 1994, March 1995).
- 39 Although the concept of record is clearly central to the Pittsburgh Project, it is somewhat difficult to locate in the literature presenting it a clearly identifiable definition of record. Records are sometimes described as "recorded transactions providing evidence" and at other times as "evidence of transactions." See Richard J. Cox, ed., *University of Pittsburgh Recordkeeping Functional Requirements Project: Reports and Working Papers* (Pittsburgh, September 1994, March 1995), *passim*. In the first formally-published mention of the Pittsburgh Project, David Bearman, who served as the consultant to the Project, defines an electronic record as "information that participates in 'transactions'." See David Bearman, "The Implications of *Armstrong v. Executive* [sic] of the President for the Archival Management of Electronic Records," *American Archivist* 56, no. 4 (Fall 1993), p. 683. Despite these slight differences in wording, the definitions are consistent in their focus on the concepts of "evidence" and "transaction" as the defining features of a record. A single, standard definition of each of these concepts does not appear to have been developed for the purposes of the Pittsburgh Project. In the glossary developed for the purposes of the UBC-MAS project, record is defined as "any document created by a physical or juridical person in the course of practical activity." Key terms used in the definition, e.g., document, juridical person, are also given separate definitions in the glossary. See Appendix C, "Third Progress Report" or view the UBC-MAS Research Project home page.

- 40 In a commentary delivered at a session on the Pittsburgh Project at the 1995 meeting of the Society of American Archivists, (Washington, D.C., 31 August 1995), P.C. Hariharan discussed some of the inadequacies of the project's method of defining functional requirements.
- 41 Personal fonds containing electronic records will be more easily accommodated in the proposed project since it will adopt the point of view of the archivist preserving the records. The point of view of the creator of the records is not relevant to the purposes of the proposed project.